

Indoor Enterprise Access Point - User Manual - MS659150M

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm/Germany

Tel. +49 2381 9452-0
FAX +49 2381 9452-100
E-Mail info@microsens.de
Web www.microsens.de

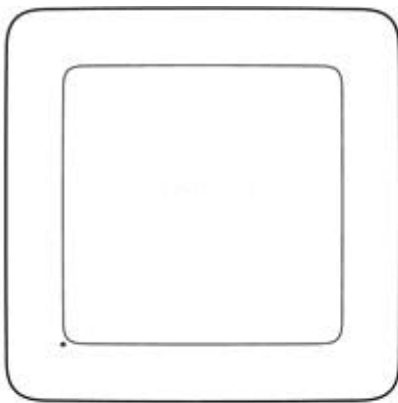
Table of Contents

1. Scope of Delivery	1
2. Getting to know your Access Point	1
2.1. LEDs	2
3. Installation	3
4. Establish AP Network	3
4.1. Connect to Network	4
4.2. Manually Assign Controller	4
4.3. Automatically Elect Controller	7
4.4. Change Password	7
5. Settings	9
5.1. Dashboard	10
5.2. Network	10
5.3. Authentication	22
5.4. Diagnostics	24
5.5. QoS	31
5.6. System Settings	33
6. Troubleshooting	38
6.1. Computer is disconnected from the Access Point.	38
6.2. Cannot find the Wi-Fi network or cannot connect to the Access Point.	38
6.3. Cannot access the Web User Interface to configure settings.	39
7. Tips & Tricks	39
7.1. Get the best Wi-Fi signal	39
7.2. Surf the Internet faster	39
7.3. Network security	39
8. Technical Specification	39
8.1. Physical	39
8.2. Wi-Fi	40

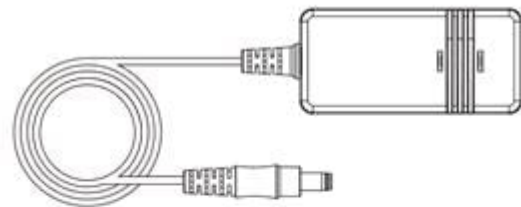
1. Scope of Delivery

The box contains the following items:

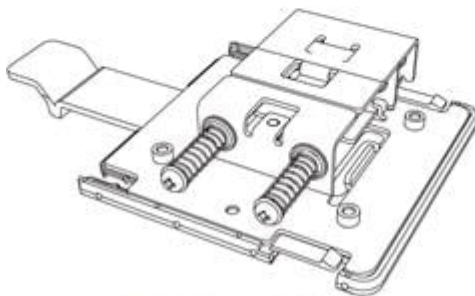
- Wi-Fi Access Point
- Ceiling installation kit
- Screw x 1 (For securing the ceiling mount bracket)
- 12V-2.5A AC Adaptor (Optional Accessory)
- Quick Start Guide



Device



12V-2.5A AC Adaptor
(Optional Accessory)



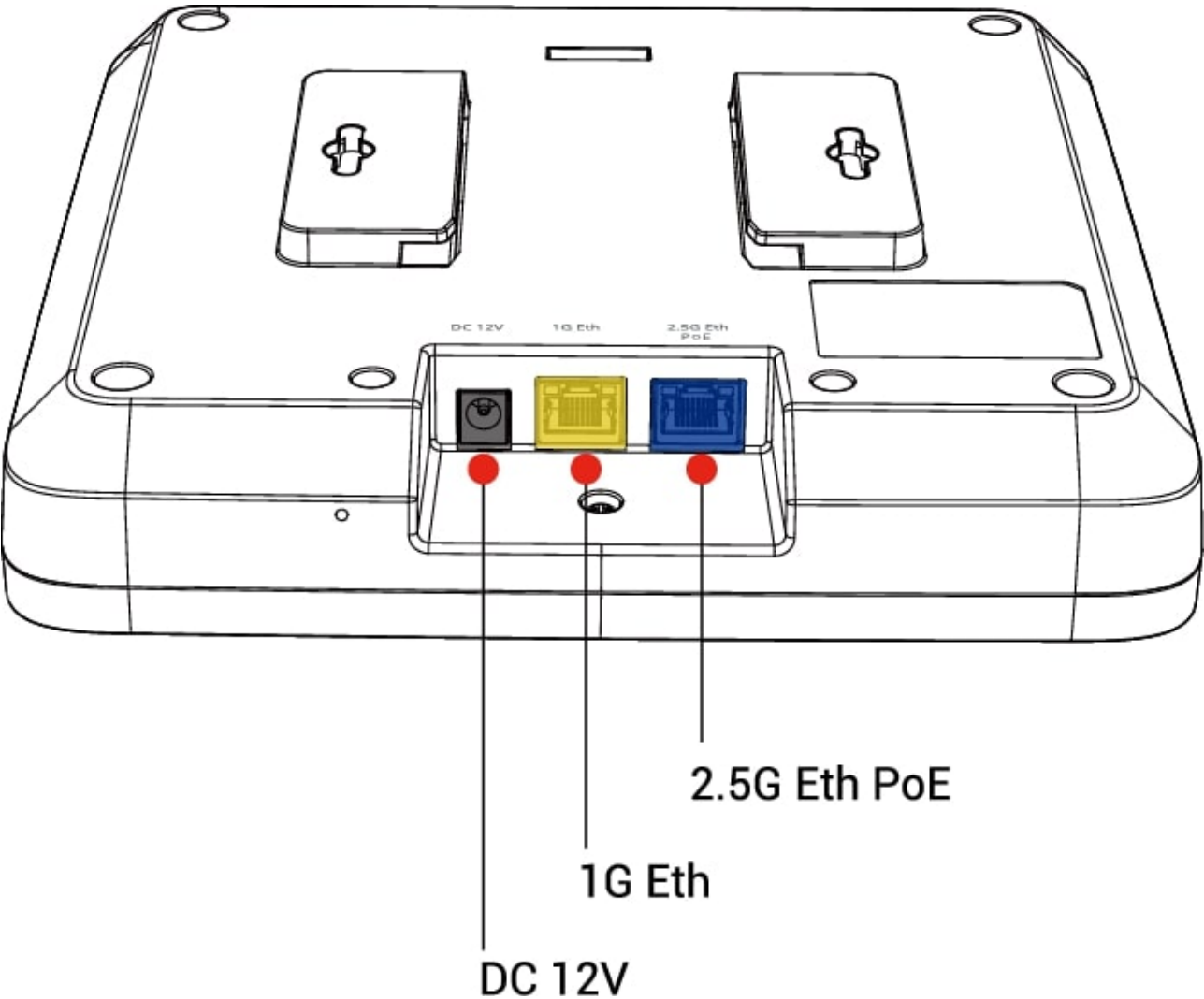
Ceiling installation kit



Screw x 1
(For securing the ceiling mount bracket)

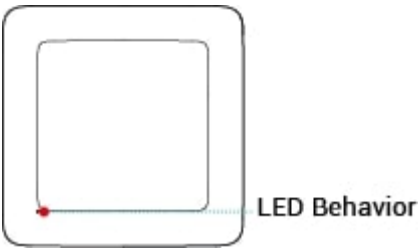
2. Getting to know your Access Point

- DC 12V: Use the AC adaptor to connect your access point to a power source.
- 1G Eth: Connect Ethernet cable for LAN (local area network) connection.
- 2.5G Eth PoE: Connect Ethernet cable for LAN (local area network) connection, or a connection with LAN and PoE+.



2.1. LEDs

The LEDs indicate the access point’s power and connection as follows:



Flashing Amber	Device is being powered on
Cyclic between Amber/Red	Firmware upgrade in process.
Solid Amber	Device has no Internet access.

Solid Green	Device is powered on and works normal.
Solid Blue	Device is Controller and normal.
Solid Red	Device is in error and cannot provide services normally.

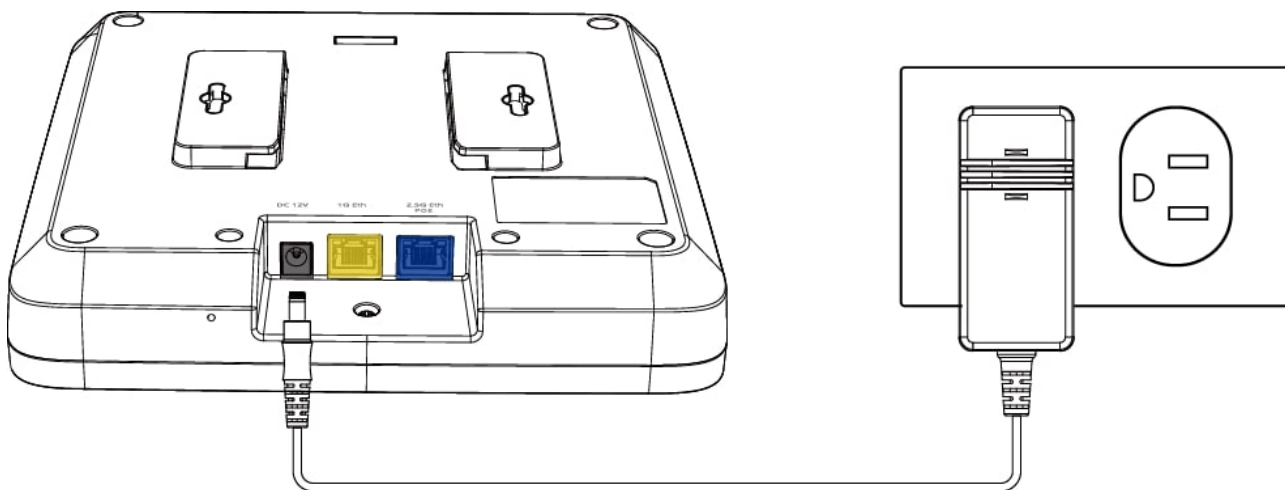
3. Installation

1. Position your access point for best performance.

Before you install and mount your access point as described in the installation guide, consider how you can position the access point for best performance. The access point lets you access your network anywhere within the operating range of your Wi-Fi network. However, the operating distance or range of your Wi-Fi connection can vary significantly depending on the physical placement of your access point. Therefore, choosing a good location is very important.

2. Set up and connect the access point to your network.

You can connect the access point to a Power over Ethernet plus (PoE+) switch in your network. The switch must be connected to a network router that is connected to the Internet. If you don't use a PoE connection, a power adapter is required for the access point as shown below:



4. Establish AP Network

An AP Network contains many access points, and they play two roles in the network: Controller and Agent. There is only one Controller in an AP Network, the others are Agents. The Controller is the AP controller of this group and it will manage Wi-Fi and lots of other functions for the entire group. The Controller is capable of controlling up to 64 access points in the same group, including itself.

In an AP Network, we first configure the Controller's Wi-Fi and other related information. For details, please go to **Network > AP Network**. After the AP Network is established, the configurations of Controller will be automatically synchronized to all Agents.

In an AP Network, some APs with the same APNID value can establish another new AP network. APNID can be configured in ACS server.

There are two ways to determine the Controller of an AP Network: manually assign Controller and automatically select Controller. For details, please go to chapters 4.2 and 4.3.

4.1. Connect to Network

To set up the access point with an Ethernet connection to your network:

1. Connect an Ethernet cable to the port on the access point.
2. Connect the other end of the Ethernet cable to a port on a switch that is connected to your network and to the Internet.

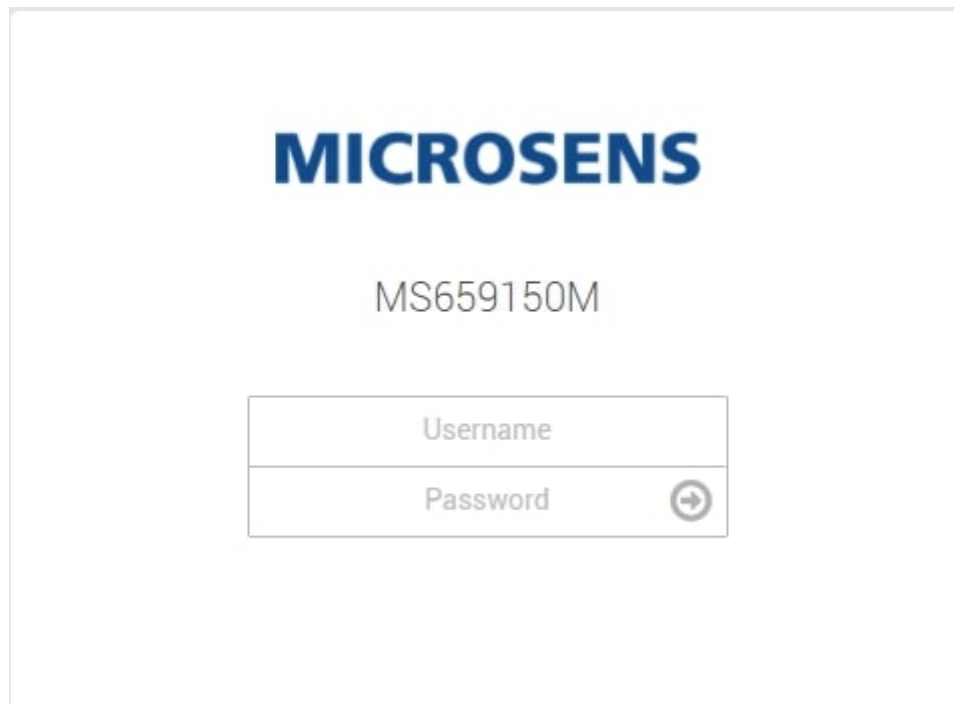


If you use a PoE connection, the port must support PoE+.

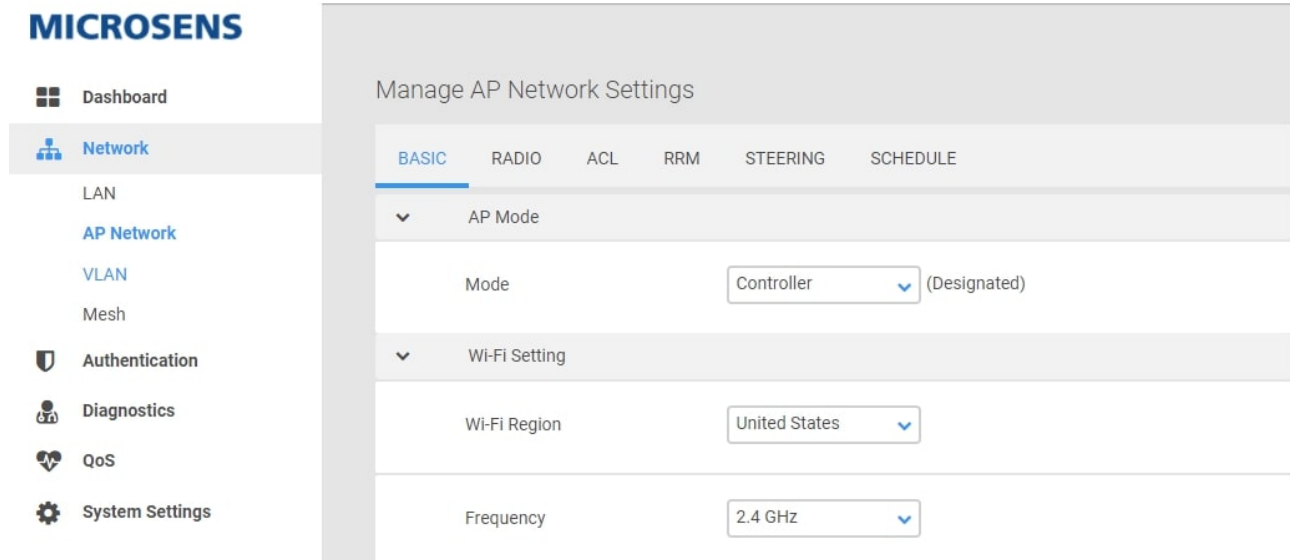
4.2. Manually Assign Controller

Configure the AP Controller

1. Place only one access point in a suitable location, and connect to the network as described in step 4.1.
2. Open a web browser and enter the URL <https://ms659150m.local>.
3. Log in to the Web UI using the default username: admin and password (Located on bottom of your access point).

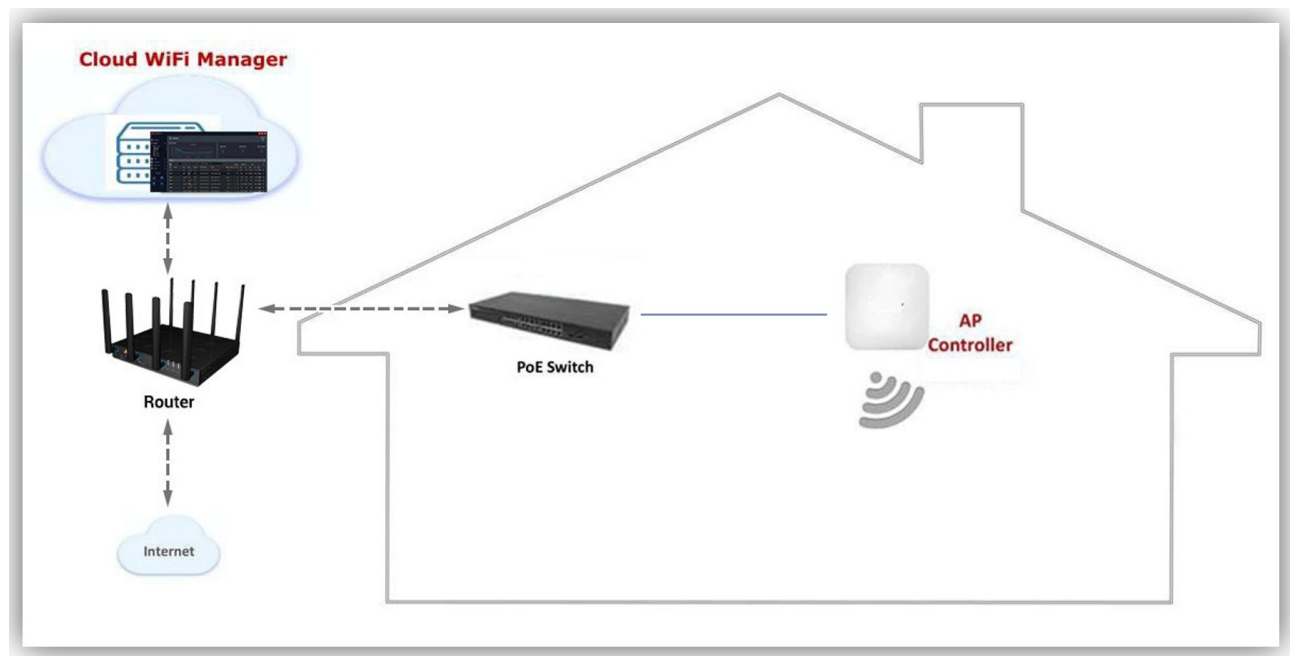


4. Go to Network > AP Network > Basic to change AP Mode to Controller, then assign it as the AP Controller of the AP network.



5. Visit the new URL <https://ms659150m-cap.local> in the browser to access to the assigned Controller.
6. Go to Network > AP Network > Basic to change Wi-Fi settings, and remember to save your settings.
7. Refer to 5. Settings in this guide for more configuration settings (optional).

Connect the AP Controller to Network



Connect Agents to the AP Network

1. Connect other access points to the same local area network to establish AP network. Record the MAC address at the bottom of each access point and relative position in AP network. When all access points have successfully connected to the network, only the Controller's LED is blue, the rest of the access points' LEDs are green.

- Go to Diagnostics > AP List, all the access points in AP network are displayed in the AP List. Find the access point by MAC address recorded in the previous step, modify its AP Name and AP Location by clicking the edit button in column Edit. Then you can quickly find an access point, view information, and personalize its radio settings.

MICROSENS

Dashboard

Network

Authentication

Diagnostics

AP List

Clients List

Events

Neighboring AP List

Spectral Scan

QoS

System Settings

Diagnostics

AP LIST

CLIENTS LIST

EVENTS

NEIGHBORING AP LIST

SPECTRAL SCAN

Search By All

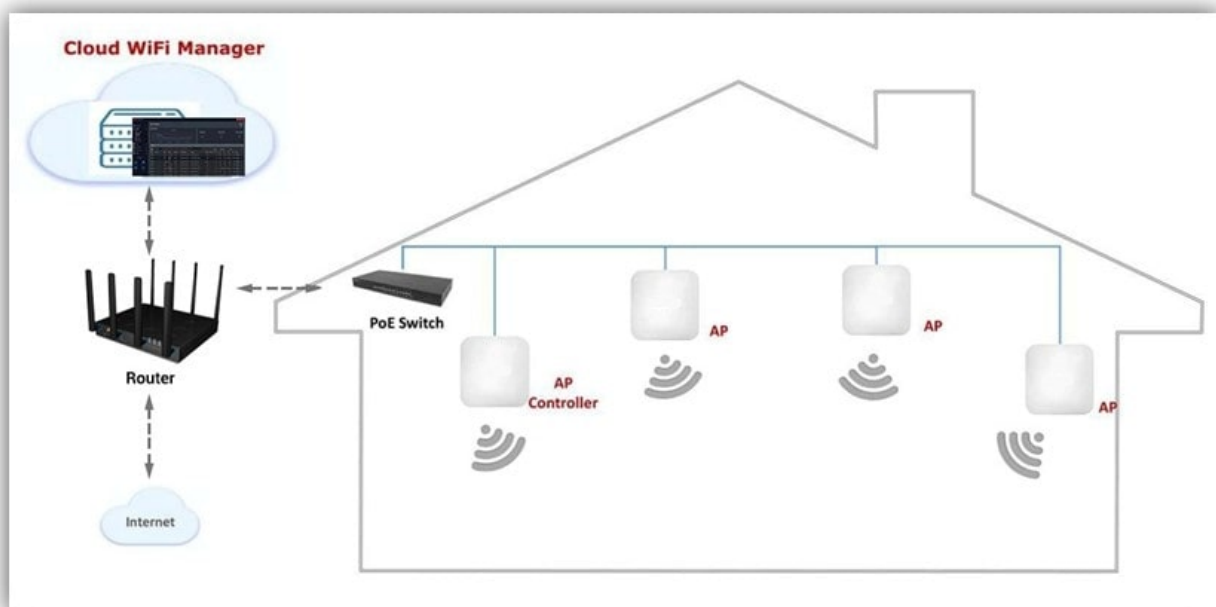
Apply

Total APs: 2

AP Name	AP MAC	IP	Radio List	AP Role	Channel	Edit
AP_Name	B4:EE:B4:EA:04:DB	192.168.0.206		Controller 11/40		
AP_Name	B4:EE:B4:EA:04:6D	192.168.0.251		Agent	6/161	

Refresh

Connect Agents to Network



If the assigned Controller is disconnected for any reason, a certain Agent in the network will be automatically elected as the new Controller in minutes to ensure the network will be back to normal immediately. Once the assigned Controller is recovered, it will act as the Controller of the AP Network again, and the automatically elected Controller will become Agent again.

4.3. Automatically Elect Controller

Connect all APs to the same Network

1. Place all access points in suitable locations, and connect them to the same local area network as described in step 4.1. Record the MAC address at the bottom of each access point and relative position.
2. The AP Network will be established in minutes and a certain access point will be automatically elected as the Controller of the AP Network. When all access points have successfully connected to the network, only the Controller's LED is blue, the rest of the access points' LEDs are green.

Configure the automatically elected Controller

1. Open a web browser and enter the URL <https://ms659150m-2.local> to access to the automatically elected Controller.
2. Log in to the Web UI using the default username: admin and password (Located on bottom of your access point).
3. Go to Network > AP Network > Basic to change Wi-Fi settings, and remember to save your settings. The Agents will synchronize Controller's Wi-Fi settings in a few minutes.
4. Go to Diagnostics > AP List, all the access points in AP network are displayed in the AP List. Find the access point by MAC address recorded in the previous step, modify its AP Name and AP Location by clicking the edit button in column Edit. Then you can quickly find an access point, view information, and personalize its radio settings.
5. Refer to 5. Settings in this guide for more configuration settings (optional).



1. When the AP Network is first established, the default AP mode of all access points is Agent, the Controller of the AP Network can be automatically elected or manually assigned.
2. When the assigned Controller exists in the network, the auto-elect mechanism will not run.
3. If the original Controller is disconnected for any reason, a certain Agent in the network will be automatically elected as the new Controller in minutes to ensure the network back to normal immediately.

4.4. Change Password

Change Access Point Password

The user will be forced to change the password when logging into access point for the first time.

Manage System Settings

System Password

Username

admin

Old Password

New Password

Confirm Password

☐ Show Password

- Username: Name used to sign in access point.
- Old Password: The default password located on bottom of the access point.
- New Password: New sign in password for access point. Its length must be 8-16 characters and a strong password.
- Confirm Password: Confirm new sign in password for access point.

Change Wi-Fi SSID/Password

The screenshot displays the 'Network' configuration page in the MICROSENS web interface. The left sidebar contains navigation links: Dashboard, Network (selected), LAN, AP Network, VLAN, Authentication, Diagnostics, and System Settings. The main content area is titled 'Network' and shows the 'Wi-Fi Setting' tab. The settings are as follows:

Setting	Value
Wi-Fi Region	Germany
Frequency Band	2.4 GHz
Clone to Other Frequency Bands	ON
Wi-Fi Network	ON
Wi-Fi Network Name (SSID)	MIC-939B1
Broadcast SSID	ON
Wi-Fi Password	faaaa564
Security Setting	WPA2-AES
Protected Management Frames	Disable
MAC Authentication	Disable
VLAN Setting	Management VLAN
Max Clients	128
Set AP Isolated	Disable
IEEE 802.11r	Enable
PMK Caching	Enable
WMM	Enable
WMM APSD	Enable
Rate Limit	Disable

At the bottom right of the settings area is a 'Cancel' button and a 'Save' button.

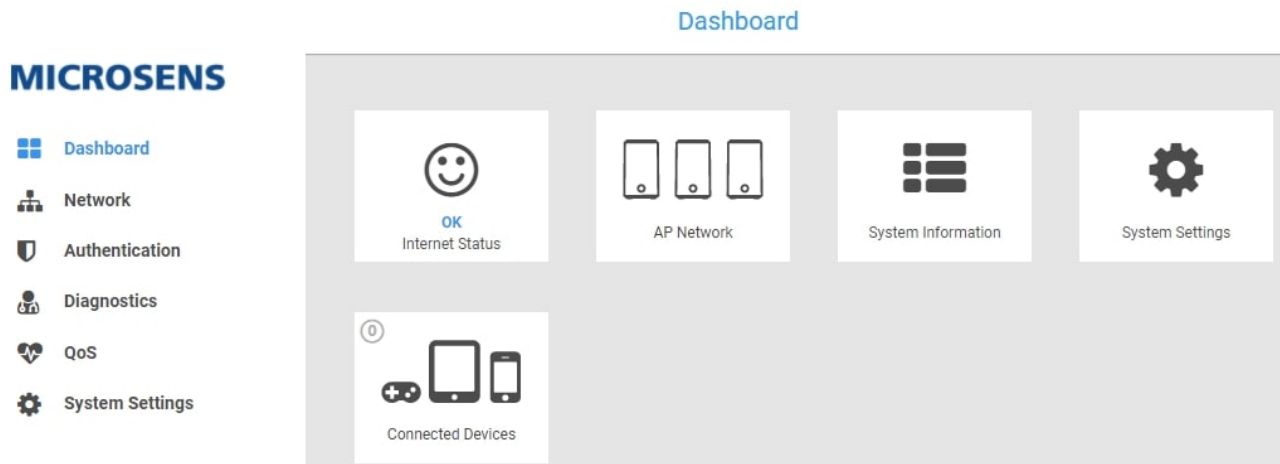
- Frequency: Select the frequency band to configure.
- Wi-Fi Network Name (SSID): This is the name of your Wi-Fi network for identification, also sometimes referred to as SSID". The default SSID is on the bottom of the access point. You can change it here, but it would no longer match the sticker on your access point.
- Wi-Fi Password: Enter your Wi-Fi password. A complex hard-to-guess key is recommended. The Wi-Fi password must be 8 characters or longer.

5. Settings

Your access point comes with an intuitive Web User Interface (Web UI) that allows you to easily setup its feature.

5.1. Dashboard

The Dashboard shows a snapshot of your network status with quick links to key features of your access point.



Select any icon on the dashboard: **Network Status**, **AP Network**, **System Information**, **System Settings**, **Connected Devices** to check more information and settings.

- **Network Status** displays the network status.
- **AP Network** takes you to **Network > AP Network > Basic**.
- **System Information** displays the access point's system information, LAN information and wireless information.
- **System Settings** takes you to **System Settings > Password & Timezone**.
- **Connected Devices** takes you to **Diagnostics > Clients List** and displays connected devices information.

5.2. Network

LAN

Click LAN button to configure the LAN connection settings:

1. LAN Connection Type: Choose the Internet Service type. There are two options: DHCP and Static IP.
2. If you select DHCP:

The screenshot shows the MICROSENS web interface. On the left is a sidebar menu with icons and labels for Dashboard, Network, LAN, AP Network, VLAN, Mesh, Authentication, Diagnostics, QoS, and System Settings. The 'Network' section is expanded, showing 'LAN' as the selected option. The main content area is titled 'Manage LAN Settings' and has a 'BRIDGE' tab selected. Under the 'BRIDGE' tab, there is a 'Basic' section. In this section, the 'LAN Connection Type' is set to 'DHCP' via a dropdown menu.

3. If you select Static IP, follow the steps below:

- IP Address: Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address.
- Subnet Mask: Specify a subnet mask. The default value is 255.255.255.0.
- Default Gateway: Enter a gateway, usually the default gateway is the same as the LAN IP.
- DNS 1 & DNS 2: Either of them indicates IP address of a DNS Server.
- Click Save.

This screenshot shows the same MICROSENS web interface as the previous one, but with the 'LAN Connection Type' set to 'Static IP'. The 'LAN IP Settings' section is expanded, showing fields for 'IP Address' (192.168.0.233), 'Subnet Mask' (255.255.255.0), and 'Default Gateway' (192.168.0.1). The 'LAN DNS Settings' section is also expanded, showing fields for 'DNS 1' (8.8.8.8) and 'DNS 2' (202.103.24.68).

AP Network

Basic

The **Basic** page allows you to configure AP Mode of access point and Wi-Fi settings for your AP Network. Your access point is dual-band and uses two Wi-Fi frequencies (2.4GHz & 5GHz) for better wireless performance on your devices.

AP Mode

The access point supports two AP Modes: Agent and Controller. No matter which mode the access point is, both 2.5G and 1G Eth port act as LAN ports.

MICROSENS

Dashboard

Network

LAN

AP Network

VLAN

Mesh

Authentication

Diagnostics

QoS

System Settings

Manage AP Network Settings

BASIC RADIO ACL RRM STEERING SCHEDULE

▼ AP Mode

Mode (Designated)

▼ Wi-Fi Setting

Wi-Fi Region

Frequency

Wi-Fi Settings

The screenshot shows the 'Network' configuration page for a MICROSENS device. The left sidebar contains navigation links: Dashboard, Network (selected), LAN, AP Network, VLAN, Authentication, Diagnostics, and System Settings. The main content area is titled 'Wi-Fi Setting' and contains the following configuration options:

- Wi-Fi Region: Germany (dropdown)
- Frequency Band: 2.4 GHz (dropdown)
- Clone to Other Frequency Bands: ☒ ON
- Wi-Fi Network: ☒ ON
- Wi-Fi Network Name (SSID): MIC-939B1
- Broadcast SSID: ☒ ON
- Wi-Fi Password: faaaa564
- Security Setting: WPA2-AES (dropdown)
- Protected Management Frames: Disable (dropdown)
- MAC Authentication: ☐ Enable ☒ Disable
- VLAN Setting: Management VLAN (dropdown)
- Max Clients: 128
- Set AP Isolated: ☐ Enable ☒ Disable
- IEEE 802.11r: ☒ Enable ☐ Disable
- PMK Caching: ☒ Enable ☐ Disable
- WMM: ☒ Enable ☐ Disable
- WMM APSD: ☒ Enable ☐ Disable
- Rate Limit: ☐ Enable ☒ Disable

At the bottom right of the settings area is a circular icon with a grid pattern. At the bottom of the page are 'Cancel' and 'Save' buttons.

Steps to set up the basic Wi-Fi settings:

1. Wi-Fi Region: Select the region to configure.
2. Frequency: Select the frequency band to configure.
3. Clone to Other Frequency Bands: Whether to sync the Wi-Fi Network configuration to 2.4G/5G.
4. Wi-Fi Network: Enable or disable this Wi-Fi band.
5. Wi-Fi Network Name (SSID): This is the name of your Wi-Fi network for identification, also sometimes referred to as "SSID". The maximum length of the SSID is 32 characters.
6. Broadcast SSID: Unable to search for SSID when is OFF.
7. Wi-Fi Password: Enter your Wi-Fi password. A complex, hard-to-guess key is recommended. The Wi-Fi password must be 8 characters or longer.

8. Security Setting: WPA2 personal is the default setting and the most secure. Security can be disabled by selecting None but this is not recommended.
9. MAC Authentication: Enable or disable MAC RADIUS authentication.
10. VLAN Setting: Select VLAN configuration from Network > VLAN.
11. Max Clients: The maximum number of clients connected to Wi-Fi.
12. Set AP Isolated: Clients connected to the same Wi-Fi Network can communicate with each other when disable.
13. IEEE 802.11r: Enable or disable fast roaming function.
14. WMM: Deployment of WMM will deliver useful QoS functionality for services such as voice over 802.11 and streaming media.
15. WMM APSD: Enable/disable automatic power save delivery.
16. Rate Limit: Enable/disable SSID related rate limit.
17. Click Save.

RADIO

The Radio page allows you to configure radio settings for your access point's Wi-Fi. You can edit radio settings for 2.4GHz or 5GHz frequency bands by clicking drop-down menu.

BASIC	RADIO	ACL	RRM	STEERING	SCHEDULE
-------	--------------	-----	-----	----------	----------

Frequency	2.4 GHz
-----------	---------

▼	Setting
---	---------

Radio	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Mode	n
Channel Bandwidth	20 MHz
Control Channel	Auto
	Current Channel : 11
Tx Bursting	Enable
Tx Power Adjustment	100%
OBSS RSSI	-61
Beacon Interval	100
HT AMPDU Factor	65535
VHT AMPDU Factor	1048575

Steps to set up the radio settings:

1. Frequency: Select the frequency band to configure.
2. Radio: Enable or disable this radio.
3. Wireless Mode: Select the wireless standard used for the access point's Wi-Fi.
4. Channel Bandwidth: The preferred channel bandwidth to be used.
5. Control Channel: Select a wireless radio channel or use the default "Auto" setting from the drop-down menu. Changing radio channel can improve Wi-Fi signal depending on how crowded the channel is with other radio signals and interference.

6. Tx Bursting: Enable TX Burst function to increase the transmission speed of devices.
7. Tx Power Adjustment: Indicates the current transmit power level as a percentage of full power.
8. OBSS RSSI: Received Signal Strength Indication, measured in dBm.
9. Beacon Interval: Beacon Interval means the period of time between one beacon and the next one. The default value is 100 (the unit is millisecond, or 1/1000 second). Lower the Beacon Interval to improve transmission performance in unstable environment or for roaming clients, but it will be power consuming.
10. HT AMPDU Factor: Enables or disables Tx AMPDU aggregation for the entire interface. Receiving aggregate frames will still be performed, but no aggregate frames will be transmitted if this is disabled.
11. VHT AMPDU Factor: Set VHT capability field, Maximum A-MPDU length exponent. Value range is 0 to 7. Maximum A-MPDU length exponent indicates the maximum length of A-MPDU that the station can receive.
12. Click Save.

ACL

Access Control List (ACL) can accept or reject devices with one or more specified MAC addresses to connect to the wireless network.

The screenshot shows the ACL configuration page with the following elements:

- Navigation tabs: BASIC, RADIO, **ACL**, RRM, STEERING, SCHEDULE.
- Frequency: 5 GHz (dropdown menu).
- Access Control List (expanded section):
 - Wi-Fi Network Name (SSID): MS659150-8DB
 - Client ACL: ☒ Enable, ☐ Disable
 - MAC Filter Mode: Reject (dropdown menu)
 - MAC Filter List (Maximum: 32):
 - MAC Address: 1C:69:7A:C5:DD:D2
 - Actions: Edit (pencil icon), Delete (minus icon)
 - Add Rule button (+ icon)

Steps to set up the ACL:

1. Frequency: In the frequency field, select the frequency band that you want to use for the

ACL settings.

2. Wi-Fi Network Name: Name for a Wi-Fi network, which is less than 32 characters.
3. Enable MAC Filter: Enable MAC filter or disable.
4. MAC Filter Mode: Select Accept to allow devices in the MAC filter list to associate to the access point, select Reject to prevent devices in the MAC filter list from associating to the AP.
5. MAC Filter List: Enter the MAC address of the wireless device. MAC filtering let users either limit specific MAC addresses from associating with the AP, or specifically indicates which MAC addresses can associate with the AP.
6. Click Save.

RRM

RRM (Radio Resource Management), contains functions as follows:

BASIC	RADIO	ACL	RRM	STEERING	SCHEDULE
Transmit Power Control					
Mode		<input type="radio"/> Auto <input type="radio"/> On Demand Optimize Power Instantly <input checked="" type="radio"/> Fixed 100% ▼			
Power Threshold		<input type="text" value="-70"/> dBm (Min: -80, Max: -50)			
Dynamic Channel Assignment					
DCA on 2.4GHz		<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
DCA on 5GHz		<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Coverage Hole Detection and Mitigation					
Coverage Hole Detection		<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
RSSI Threshold		<input type="text" value="-80"/> dBm (Min: -90, Max: -60)			
Minimum Count of Client in Coverage Exception		<input type="text" value="3"/> (Min: 1, Max: 100)			

Transmit Power Control: Support three modes, namely Auto, On Demand and Fixed.

- Auto Mode: AP Controller will periodically adjust and optimize the Tx Power of all APs in the network, the default interval is 10 minutes.
- On Demand Mode: AP Controller will not synchronize Tx Power to Agents. If you want to optimize the Tx Power of the entire network, click the "optimize power instantly" button to optimize instantly only once.
- Fixed Mode: AP Controller will synchronize fixed Tx Power (100%, 75%, 50%, 25%) to all Agents.
- Power Threshold: Used for automatic optimization algorithms, the default value is -70dBm.

Dynamic Channel Assignment: Dynamically select channels with low interference to improve network performance.

- DCA on 2.4GHz: Enable or disable the function on 2.4GHz.
- DCA on 5GHz: Enable or disable the function on 5GHz.

Coverage Hole Detection and Mitigation: The function is to detect coverage holes, and mitigate them (if possible and wise) by increasing power.

- Coverage Hole Detection: Enable or disable the function.
- RSSI Threshold: Used to judge the connection quality of the Wi-Fi terminal, the default value is -80dBm. If the network signal coverage requirement is strong, the value can be increased appropriately.
- Minimum Count of Client in Coverage Exception: The minimum number of clients that must be in a coverage hole before mitigation can be considered. The default value is 3.

STEERING

AP steering: Load Balancing Steering-Enable clients such as mobile phone and notebooks can be evenly distributed to AP as far as possible to improve overall network utilization.

Mobility Steering: Enable clients such as mobile phone and notebooks to connect to the nearest AP as far as possible to obtain better signal and connection speed.

Band steering: lets the access point identify the Wi-Fi devices that are dual-band capable and steer those devices to the 2.4 GHz or 5 GHz band of a Wi-Fi network.

BASIC RADIO ACL RRM **STEERING** SCHEDULE

▼ AP Steering

AP Steering ☐ Enable ☒ Disable

▼ Band Steering

Band Steering ☒ Enable ☐ Disable



To enable AP Steering you must enable Band Steering.

SCHEDULE

The Schedule feature allows you to configure to turn on or off a certain Wi-Fi Network within a set time period.

BASIC RADIO ACL RRM STEERING **SCHEDULE**

SSID MIC-939B1 ▼

▼ Schedule

Wireless Scheduler ☒ Enable ☐ Disable

Effective Working Day ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri

Time in Working Day 08 : 00 ~ 22 : 10 ☐ All Day

Effective Non-Working Day ☒ Sat ☒ Sun

Time in Non-Working Day : ~ : ☒ All Day

Steps to set Schedule

1. SSID: Select the SSID to configure.
2. Wireless Scheduler: Enable or disable wireless schedule.
3. Effective Working Day: Select working days to enable Wi-Fi.

4. Time in Working Day: Set working day time to enable Wi-Fi.
5. Effective Non-Working Day: Select non-working days to enable Wi-Fi.
6. Time in Non-Working Day: Set non-working day time to enable Wi-Fi.
7. Click Save.

VLAN

The VLAN page allows you to configure up to four VLANs. Set VLAN ID to empty means untag. The VLAN is applied to Wi-Fi Settings, for details, please go to **Network > AP Network > Basic**.

MICROSENS

- Dashboard
- Network**
 - LAN
 - AP Network
 - VLAN**
 - Mesh
- Authentication
- Diagnostics
- QoS
- System Settings

Manage VLAN Settings

VLAN

VLAN	VLAN Name	VLAN ID	VLAN Priority
1	Mangement VLAN		0
2	Custom VLAN 1	10	0
3	Custom VLAN 2	20	0
4	Custom VLAN 3	30	0

Mesh

The Mesh page allows you to configure all APs' mesh mode: standalone, root and extender.

MICROSENS

- Dashboard
- Network**
 - LAN
 - AP Network
 - VLAN
 - Mesh**
- Authentication
- Diagnostics
- QoS
- System Settings

Manage MESH Settings



AP LIST TOPOLOGY

MAC	AP Mode	Mesh Mode	Running Mode	Connection	Edit / Delete
B4:EE:B4:EA:04:DB	Controller	Root	Root	Online	
B4:EE:B4:EA:04:6D	Agent	Extender	Extender	Online	

Refresh

AP List

Display the APs' Mesh mode information. And you can edit APs' mesh mode in this page.

AP LIST TOPOLOGY					
MAC	AP Mode	Mesh Mode	Running Mode	Connection	Edit / Delete
B4:EE:B4:EA:04:DB	Controller	Root	Root	Online	
B4:EE:B4:EA:04:6D	Agent	Extender	Extender	Online	

Refresh

Standalone: Fronthaul AP only. (In this mode, AP can be controller or agent AP)

Root: Fronthaul AP + backhaul Wi-Fi AP. (In this mode, AP can be controller or agent AP)

Extender: Fronthaul AP + backhaul Wi-Fi STA. (In this mode, AP only can be agent AP)



1. Controller can only be opened in root or standalone mode, and controller can only be accessed by network cable.
2. For an AP that is already in root mode, if there is an AP in extender mode connected to it, the root mode cannot be changed.
3. If any AP is in extender mode, there must be at least one root mode AP in the network.
4. For online APs, it cannot be deleted (only offline APs will display the delete icon)
5. The interval of edit and save mesh mode must be longer than 3 min.

TOPOLOGY

Display online MESH APs' SN, IP and MAC.

APs in root or standalone mode will display on the same level.

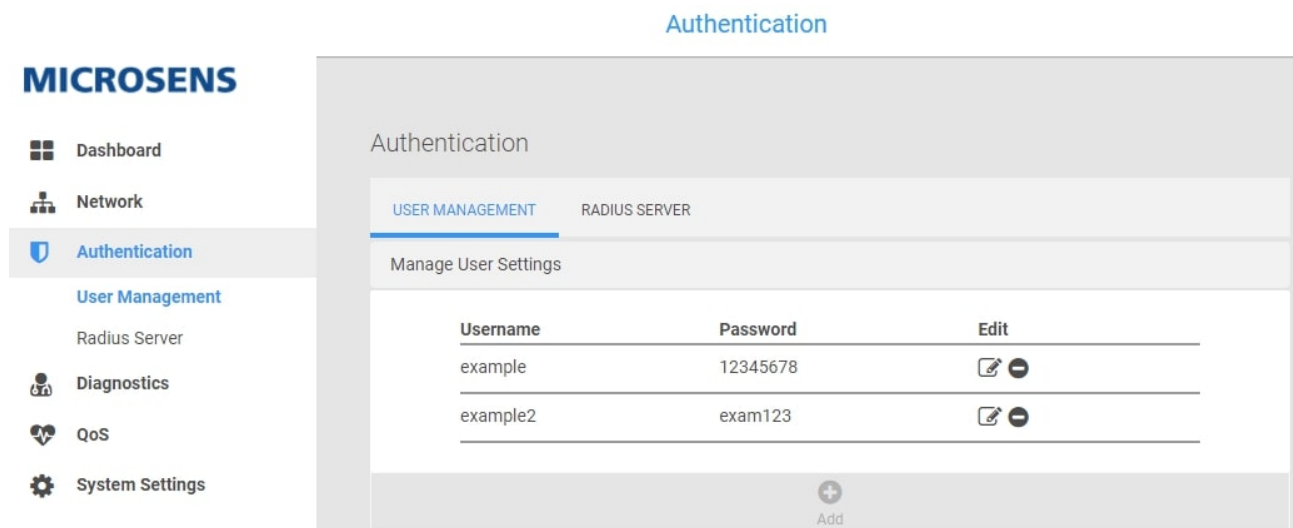
APs in extender mode will display in next level which they connected the AP in root mode.



5.3. Authentication

User Management

User management provides the configuration of radius users.



Steps to set radius user:

1. Username: Name to sign in radius server.
2. Password: Password to sign in radius server.
3. Confirm Password: Confirm password to sign in radius server.
4. Click Add.

Manage User Settings

Username

example

Password

.....

Confirm Password

.....

Cancel

Apply

Radius Server

The RADIUS server has capabilities of Authentication, Authorization, and Accounting. The user can access to network only if the RADIUS Server authenticates and authorizes the user.

For WPA2/WPA3 Enterprise security of Wi-Fi network, RADIUS server is needed.

MICROSENS

Dashboard

Network

Authentication

User Management

Radius Server

Diagnostics

QoS

System Settings

Authentication

USER MANAGEMENT

RADIUS SERVER

Manage Authentication Settings

Authentication Port

1812

Accounting Port

1813

IP Address Segment

192.168.1.0

/

24

Shared Secret

secret123

Steps to set up radius server:

1. Authentication Port: Enter UDP port on the access point that is used to access the RADIUS server. For authentication servers, the default port is 1812.
2. Accounting Port: For accounting servers, the default port is 1813.
3. IP Address: Enter the IPv4 address of the Radius Server. The access point must be able to reach the IP address.
4. Shared Secret: It's used between the access point and the RADIUS server during the authentication or accounting process.

5. Click Save.

5.4. Diagnostics

AP List

Diagnostics > AP List

Display the APs' information in AP Network, with quick links to SSID List, Radio Settings and AP Settings. And you can quickly find the relevant AP through the search function.

MICROSENS

Dashboard

Network

Authentication

Diagnostics

AP List

Clients List

Events

Neighboring AP List

Spectral Scan

QoS

System Settings

Diagnostics

AP LIST CLIENTS LIST EVENTS NEIGHBORING AP LIST SPECTRAL SCAN

Search By All **Apply** Total APs: 2

AP Name	AP MAC	IP	Radio List	AP Role	Channel	Edit
AP_Name	B4:EE:B4:EA:04:DB	192.168.0.206		Controller 11/48		
AP_Name	B4:EE:B4:EA:04:6D	192.168.0.251		Agent	6/48	

Refresh

SSID List

Display Radio, SSID, VLAN and other information of the Wi-Fi Network.

SSID List						
Radio	SSID	BSSID	VLAN	STATUS	Uplink Bandwidth(Mb/s)	Downlink Bandwidth(Mb/s)
5GHz	Microsens Gast	84:D8:1B:8B:E2:4D	No_Tag	up	0	0
5GHz	Microsens	8A:D8:1B:8B:E2:4D	10	up	504	380
5GHz	Microsens	8A:D8:1B:8B:DB:EB	20	up	0	0
5GHz	Microsens Gast	84:D8:1B:8B:DB:EB	30	up	0	0
2.4GHz	Microsens Gast	84:D8:1B:8B:DB:EA	No_Tag	up	0	0
2.4GHz	Microsens	8A:D8:1B:8B:DB:EA	10	up	0	0
2.4GHz	Microsens	8A:D8:1B:8B:E2:4C	20	up	0	0
2.4GHz	Microsens Gast	84:D8:1B:8B:E2:4C	30	up	0	0

Radio Status

The Radio Status page shows you radio information of each AP in the AP Network.

Radio Status

Frequency

2.4 GHz

Radio

Enabled

Mode

n

Control Channel

6

Channel Bandwidth

20 MHz

Tx Power

30dbm

Tx Bursting

Enabled

OBSS RSSI Threshold

-61

Beacon Interval

100

Utilization

100%

Stations

0

Tx Packets

0

Tx Bytes

0

Tx Drop_Packets

0

Tx Errors

0

Rx Packets

0

Rx Bytes

0

Rx Drop_Packets

0

Rx Errors

0

AP Settings

Allows to modify AP Name and AP Location according to the location of the AP.

AP Settings

AP Name

AP_Name

AP Location

AP_Loc

Cancel

Save

Clients List

Diagnostics > Clients List

Display the Wi-Fi clients' information connected to the AP Network, with quick links to Clients Info in detail by clicking Clients MAC. And you can quickly find the relevant clients through the search function.

MICROSENS

Dashboard

Network

Authentication

Diagnostics

AP List

Clients List

Events

Neighboring AP List

Spectral Scan

QoS

System Settings

Diagnostics

AP LIST

CLIENTS LIST

EVENTS

NEIGHBORING AP LIST

SPECTRAL SCAN

Search By

All

Apply

Total Clients: 2

Clients MAC	AP Name	AP MAC	SSID	BSSID	Radio	Channel
10:A5:1D:00:59:1A	AP_Name	B4:EE:B4:EA:04:DB	Askey-838DB	B4:EE:B4:EA:04:DE	5GHz	48
02:A2:D3:51:A6:2B	AP_Name	B4:EE:B4:EA:04:DB	Askey-838DB	B4:EE:B4:EA:04:DE	5GHz	48

Refresh

Clients Info

Display the details of the client's connection information.

Clients Info

VLAN	Association Time	RSSI	Uplink Rate(Mb/s)	Downlink Rate(Mb/s)
Untagged	2022-07-21 10:28:07	-42dBm	560.00	560.00

Events

Record Controller, Agent status, Wi-Fi client connection status, etc. And you can quickly find the relevant events log through the search function.

Diagnostics

AP LIST

CLIENTS LIST

EVENTS

NEIGHBORING AP LIST

SPECTRAL SCAN

Search By

Apply

Event Logs

```

Wed Jul 20 16:08:08 2022 B4:EE:B4:EA:04:DB cmsg_mesh_mode_changed lapp
Wed Jul 20 16:08:18 2022 B4:EE:B4:EA:04:DB cmsg_DE_CAP_up b4:ee:b4:ea:04:db
Wed Jul 20 16:08:41 2022 B4:EE:B4:EA:04:DB cmsg_DE_RE_up B4:EE:B4:EA:04:6D
Wed Jul 20 16:33:41 2022 B4:EE:B4:EA:04:DB cmsg_mesh_apmesh_mode_changed web
Wed Jul 20 16:33:43 2022 B4:EE:B4:EA:04:DB cmsg_mesh_ucicfg_change web
Wed Jul 20 16:33:44 2022 B4:EE:B4:EA:04:6D cmsg_mesh_apmesh_mode_changed lapp-ext
Wed Jul 20 16:34:10 2022 B4:EE:B4:EA:04:DB cmsg_DE_RE_down B4:EE:B4:EA:04:6D
Wed Jul 20 16:35:29 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_assoc C6:EE:B4:EA:04:70
Wed Jul 20 16:35:50 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_disassoc C6:EE:B4:EA:04:70
Wed Jul 20 16:35:50 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_assoc C6:EE:B4:EA:04:70
Wed Jul 20 16:36:04 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_disassoc C6:EE:B4:EA:04:70
Wed Jul 20 16:36:34 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_assoc C6:EE:B4:EA:04:70
Wed Jul 20 16:37:05 2022 B4:EE:B4:EA:04:DB cmsg_DE_RE_up B4:EE:B4:EA:04:6D
Wed Jul 20 16:37:16 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_disassoc 56:64:1A:7E:41:FC
Wed Jul 20 16:37:34 2022 B4:EE:B4:EA:04:6D cmsg_DE_STA_disassoc 0A:CF:B8:B1:F6:B2
Wed Jul 20 16:37:47 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_disassoc 56:64:1A:7E:41:FC
Wed Jul 20 16:37:54 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_assoc 56:64:1A:7E:41:FC
Wed Jul 20 16:41:21 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_assoc 0A:CF:B8:B1:F6:B2
Wed Jul 20 16:43:57 2022 B4:EE:B4:EA:04:DB cmsg_DE_STA_disassoc 56:64:1A:7E:41:FC

```

Refresh

Neighbouring AP List

Displays nearby Wi-Fi Network information. And you can quickly find the relevant Wi-Fi Networks through the search function.

CLIENTS LIST EVENTS NEIGHBORING AP LIST SPECTRAL SCAN					
Search By		All ▼	<input type="text"/>	Apply	Total Neighboring APs: 16
Band	SSID	BSSID	Channel	Signal Strength	▲
5GHz	Microsens Gast	84:D8:1B:8B:E2:4D	40	-72	
5GHz	Microsens	8A:D8:1B:8B:E2:4D	40	-73	
5GHz	Microsens	8A:D8:1B:8B:DB:EB	44	-73	
5GHz	Microsens Gast	84:D8:1B:8B:DB:EB	44	-74	
5GHz	Prometheus_5G	A4:2B:B0:A3:AD:B0	36	-86	
2.4GHz	Prometheus	A4:2B:B0:A3:AD:AE	1	-63	
2.4GHz	Microsens Gast	84:D8:1B:8B:DB:EA	6	-65	
2.4GHz	Microsens	8A:D8:1B:8B:DB:EA	6	-65	
2.4GHz	Microsens	8A:D8:1B:8B:E2:4C	11	-75	
2.4GHz	Microsens Gast	84:D8:1B:8B:E2:4C	11	-75	
2.4GHz	Puro	C4:93:00:02:DC:81	6	-76	▼
Refresh					

Spectral Scan

Scan the selected Wi-Fi channel.

Diagnostics

AP LIST

CLIENTS LIST

EVENTS

NEIGHBORING AP LIST

SPECTRAL SCAN

Scan Channels:

☒ 1

☒ 6

☒ 11

☒ 36

☒ 40

☒ 44

☒ 48

☐ 52

☐ 56

☐ 60

☐ 64

☐ 100

☐ 104

☐ 108

☐ 112

☐ 116

☐ 120

☐ 124

☐ 128

☐ 132

☐ 136

☐ 140

☐ 144

☒ 149

☒ 153

☒ 157

☒ 161

☒ 165

Start Scan

Scan Result

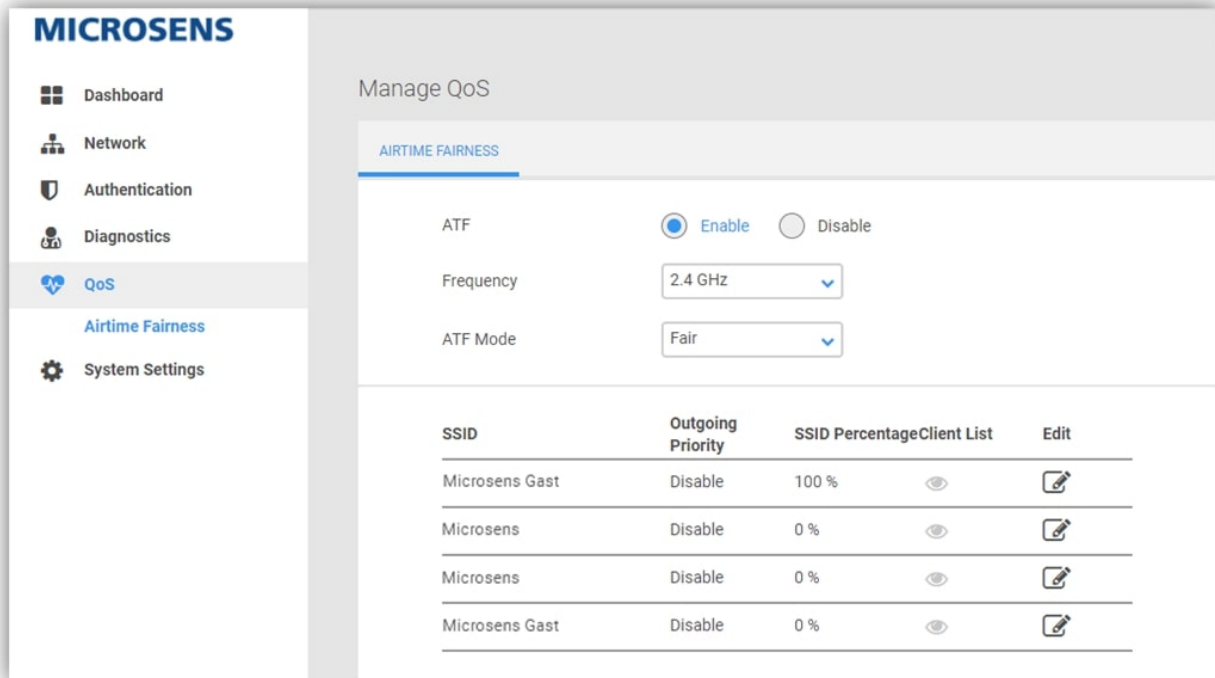
No content to display !

Refresh

5.5. QoS

Airtime Fairness

Airtime Fairness is a feature that boost the overall network performance by sacrifice a little bit of network time on your slowest devices.



Steps to set ATF

1. ATF: Enable or disable. ATF require primarily focuses on scheduling fairness for transmission of traffic from Access Point (AP), and efficient Wi-Fi bandwidth utilization.
2. Frequency: Select the frequency band that you want to use for the ATF settings.
3. ATF Mode: Strict and fair algorithm, which are mutually exclusive. Strict algorithm follows strict airtime allocation as configured by the user and does not try and utilize any unused bandwidth. Fair algorithm guarantees the configured airtime in congested environments and it also utilizes any unused bandwidth.
4. Select SSID and click Edit button.
5. SSID Percentage: Set the percentage of SSID which will be used for ATF control.
6. Current Client List: Select client by MAC address.
7. Client MAC: Manually enter a client MAC address
8. Percentage: Set the percentage for client which will be used for ATF control.
9. Click Confirm.

Settings

SSID

MIC-939B1

Outgoing Priority

Disable

SSID Percentage

80

%

Clients Setting:

Current Client List

02:a2:d3:51:a6:2b

Client MAC

02:a2:d3:51:a6:2b

Percentage

60

%

Add Client

Cancel

Confirm

5.6. System Settings

Password & Timezone

This page allows you to configure access point's login password and time settings.

MICROSENS

Dashboard
Network
Authentication
Diagnostics
QoS
System Settings
 Password & Timezone
 Reboot
 Configuration & Reset
 Firmware
 SNMP
 Cloud

PASSWORD & TIMEZONE REBOOT CONFIGURATION & RESET FIRMWARE SNMP CLOUD

System Password

Username: admin

Old Password:

New Password:

Confirm Password: ☐ Show Password

Time Zone

Time Zone: Auto

Miscellaneous

Auto Logout: 5 Minutes (Disable:0)

NTP Server (Maximum : 5)

NTP Server	Edit / Delete
time.nist.gov	
time-d-g.nist.gov	
time-e-g.nist.gov	
time-d-b.nist.gov	
time-e-b.nist.gov	

+
Add

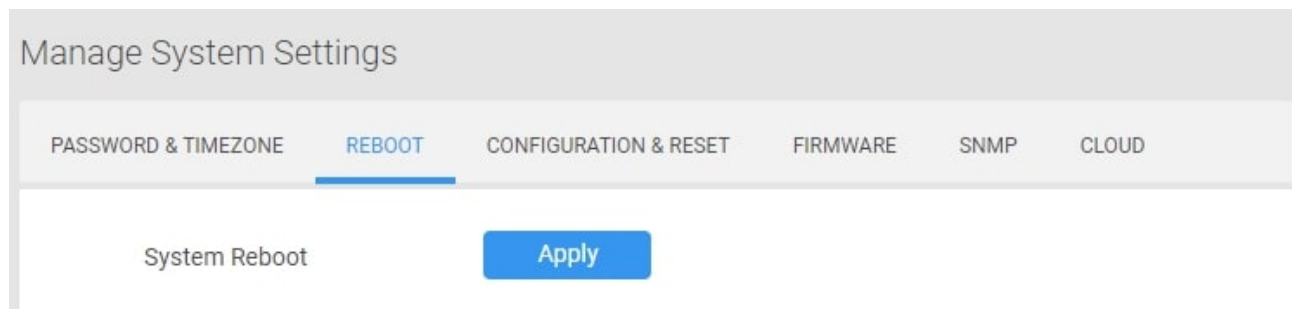
Steps to set Password & Timezone:

1. Username: Name used to sign in access point.
2. Old Password: Old sign in password for access point.
3. New Password: New sign in password for access point. Its length must be 8-16 characters and a strong password.
4. Confirm Password: Confirm new sign in password for access point.
5. Time Zone: The default value is Auto.
6. Auto Logout: Auto sign out after a specified period of time.

7. NTP Server: DNS of a NTP (Network Time Protocol) server.
8. Click Save.

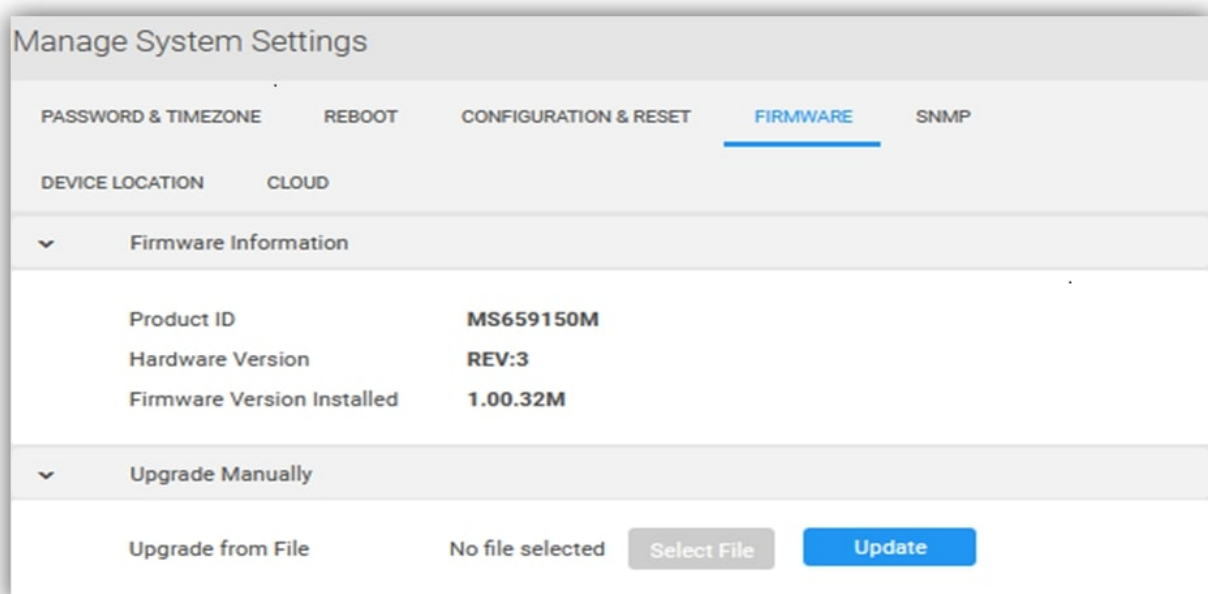
Reboot

Reboot the access point by press **Apply** button.



Firmware

The Firmware page displays your access point's firmware version and hardware version information and can upload firmware manually when select a valid firmware to update it.



Configuration & Reset

The Configuration & Reset page enables you to save/upload the access point's current settings as a file to your local computer, or upload your access point to previously saved settings by loading a backed up file. You can also reset the access point back to factory default settings. If the access point malfunctions or is not responding, then it is recommended that you first **reboot the device** (press the reset button for 1 second), and if still experiencing problems **reset the device back to its factory default settings**. You can reset the access point back to its default settings using the Reset button on the back of the access point (press and hold for 5+ seconds).

Manage System Settings

PASSWORD & TIMEZONE REBOOT **CONFIGURATION & RESET** FIRMWARE SNMP CLOUD

Configuration

Save to File **Save**

Restore from File No file selected **Select File** **Upload**

Reset

Reset to Default **Reset to Default**

Steps to Save to File, Restore from File and Reset to Default:

1. Click Save, and then the browser will automatically download access point's setting files.
2. Click Restore from File to select setting file, then click Upload button, this will make the access point to upload the configuration file to device and applied the configuration file settings.
3. Click Reset to Default, this will reset all settings to factory default settings.

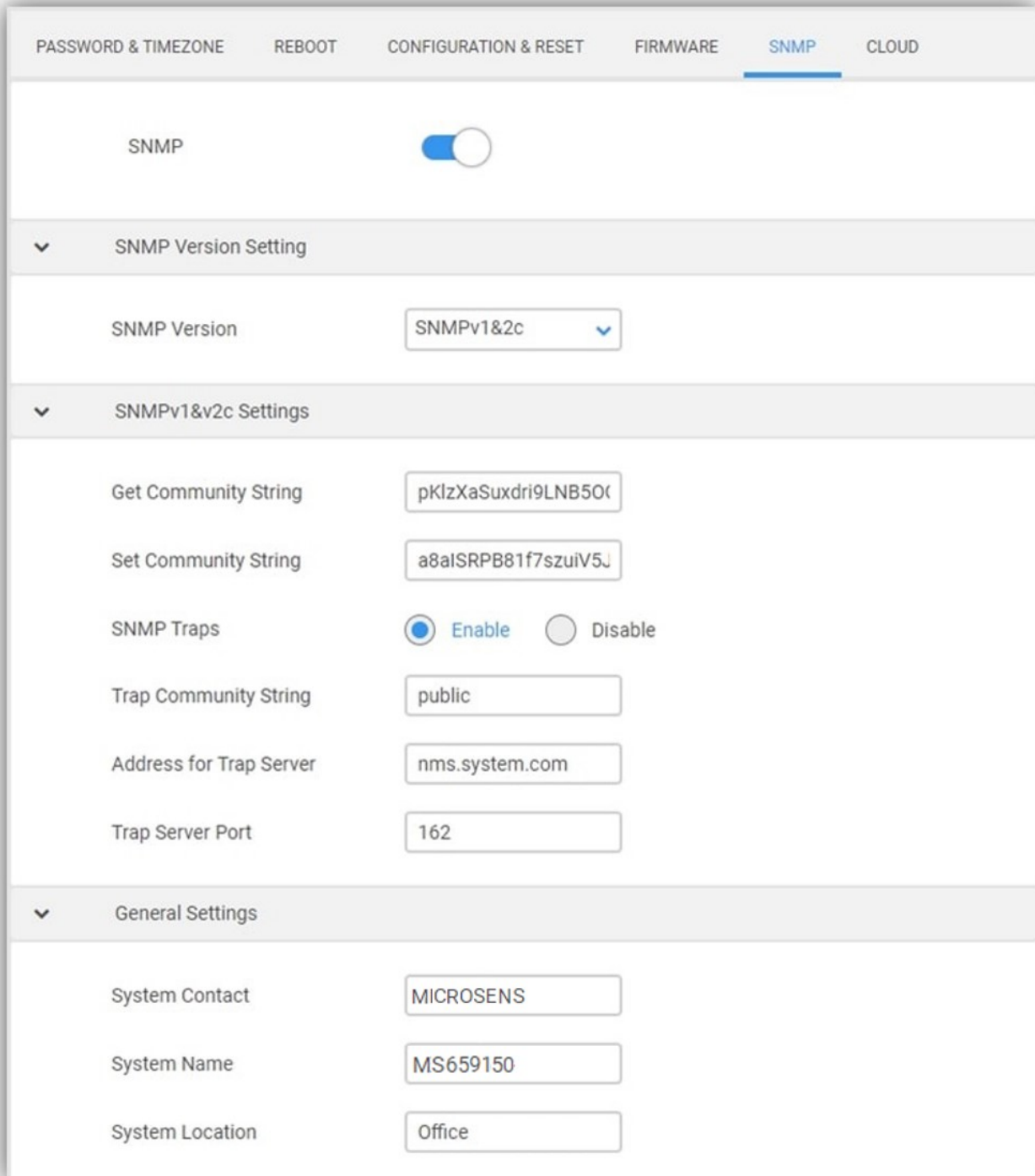


1. Reboot the device – press the reset button for 1 second;
2. Reset the device back to its factory default settings – press and hold for 5+ seconds.

SNMP

Simple Network Management Protocol (**SNMP**), The SNMP management station uses the Get-Request message to retrieve information from the network device that has the SNMP agent, and the SNMP agent responds with the Get-Response message. Get-Next- Request is used in combination with Get-Request to query column elements in a specific table object. By default, SNMP is disabled.

MIB Browser, which can connect to the network device of the specified IP, and obtain the OID value of the specified MIB through the SNMP protocol, supporting v1, v2, and v3 versions.



PASSWORD & TIMEZONE REBOOT CONFIGURATION & RESET FIRMWARE **SNMP** CLOUD

SNMP ☒

▼ SNMP Version Setting

SNMP Version

▼ SNMPv1&v2c Settings

Get Community String

Set Community String

SNMP Traps ☒ Enable ☐ Disable

Trap Community String

Address for Trap Server

Trap Server Port

▼ General Settings

System Contact

System Name

System Location

Steps to set SNMPv1&v2c Settings:

1. SNMP: Enable or disable SNMP function.
2. SNMP Version: Choose SNMPv1&v2 or SNMPv3.
3. Get Community String: The community name with read permission.
4. Set Community String: The community name with write permission.
5. SNMP Traps: Enable or disable SNMP Traps.

6. Trap Community String
7. Address for Trap Server
8. Trap Server Port
9. System Contact: Describe the information of contact who manages this access point.
10. System Name: Describe the name to identify the device.
11. System Location: Describe the location of the access point with SNMP Agent enabled.

▼

SNMPv3 Settings

Authentication Type

MD5-DES

▼

User Name

myname

Password

.....

☐ Show Password

Private Password

.....

☐ Show Password

Context Name

SNMPv3 Traps

☒ Enable ☐ Disable

Address for SNMPv3 Trap Server

nms.system.com

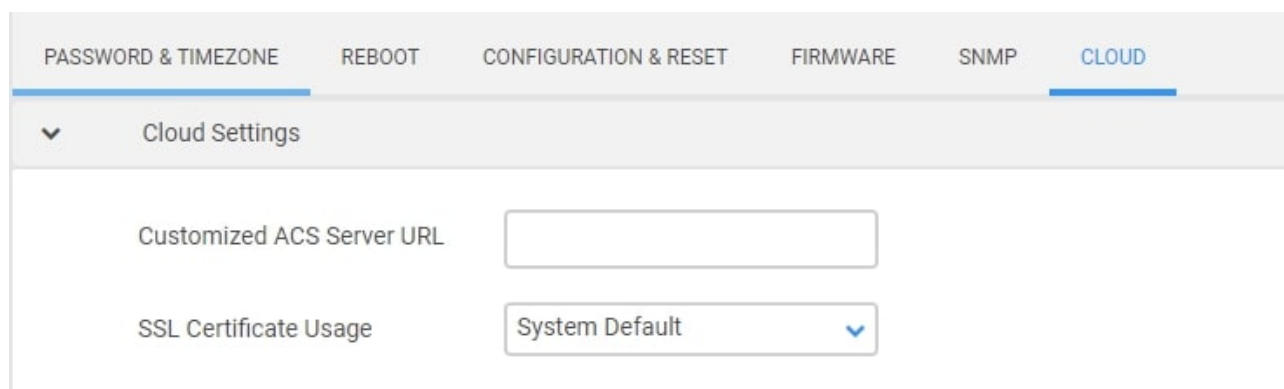
SNMPv3 Trap Server Port

162

Steps to set SNMPv3 Settings:

1. Authentication Type: Authentication and Encryption type of SNMPv3 messages. Support three security levels noAuthnoPriv, AuthNoPriv and AuthPriv.
2. User Name
3. Password: The password of authentication.
4. Private Password: The password of encryption.
5. Context Name: Used to determine the MIB view of the SNMP unique identifier to the managed device.
6. SNMPv3 Traps: Enable or disable SNMPv3 Traps.
7. Address for SNMPv3 Trap Server
8. SNMPv3 Trap Server Port

Cloud



The **Cloud** page allow you to set ACS server URL access through ACS Server. Customized ACS Server URL: Input EMP Cloud server or other ACS Server's URL SSL Certificate Usage System Default: ACS Server's default SSL Certificate Disable: ACS Server has no authentication Customized: ACS Server provides Plain Text of Root CA, Plain Text of Device Certificate and Plain Text of Device Private Key.

6. Troubleshooting

If you are having problems with your access point, try these basic steps in this section before looking for further solutions.

6.1. Computer is disconnected from the Access Point.

Your computer might have lost the connection to the access point due to interference, system updates, or any number of reasons. If you're not connected, reconnect to the access point's Wi-Fi and make sure the password is correct, or use an Ethernet cable to connect directly to the access point's LAN port. Follow the steps in **4. Establish AP network** for more help.

6.2. Cannot find the Wi-Fi network or cannot connect to the Access Point.

If you can't see your access point's Wi-Fi when scanning available networks, or if you can't establish a connection, try the following:

- Refresh the list of available Wi-Fi networks on your device.
- Switch the access point off and back on again with the power switch.
- Move the access point closer to your device, or move your device closer to the access point.
- Restart your device or computer.

If you still cannot find the Wi-Fi network or establish a connection, then try to reset your access point back to factory default settings. To do this, press and hold the reset button on the back of the access point for at least 5 seconds and wait for the access point to restart. Then repeat the connection process as described in **4. Establish AP network**.

6.3. Cannot access the Web User Interface to configure settings.

If you cannot access the Web UI, it might be an issue with your device or computer's proxy or IP address settings. Make sure that proxy settings are disabled and that your device or computer can be allocated an IP address on the network by the access point's DHCP server. You'll need to check the support for your device or computer's operating system e.g. Windows, macOS, for detailed instructions how to do this.

7. Tips & Tricks

7.1. Get the best Wi-Fi signal

Where you place the access point can affect your wireless coverage. For the best Wi-Fi performance, your access point needs open spaces, away from walls, obstructions and heavy-duty appliances or electronics.

7.2. Surf the Internet faster

Have you thought of changing your network frequency band to enjoy a faster connection? Your access point is dual-band (2.4GHz & 5GHz), so you will likely get better speed by switching to the 5GHz band instead of the more commonly used and congested 2.4GHz band. Make sure your 5 GHz Wi-Fi is active at Network > AP Network in the access point's Web UI, and connect your Wi-Fi device or computer to the 5GHz band instead of 2.4GHz.

7.3. Network security

Your access point is pre-set with the recommended WPA2 security type, but you should immediately change the default Wi-Fi password, as well as the Web UI login password. You can do so at Network > AP Network and System Settings > Password & Timezone in the Web UI. It is not recommended to change Wi-Fi security type: WPA2 with AES is the most secure. And it is never recommended to disable Wi-Fi security (no security type), this means your network is open and anybody within range can connect by Wi-Fi.

8. Technical Specification

8.1. Physical

CPU	<ul style="list-style-type: none">Qualcomm IPQ8072A (Hawkeye) with Quadcore 2.2Gbps A53
Chip Set	<ul style="list-style-type: none">Main SoC: Qualcomm IPQ8072A, Quad A53 @ 2.2GHzMemory: 1GB DDR4, 8GB eMMC
RF Functions	<ul style="list-style-type: none">DBDC 802.11ax Wi-Fi with 8 spatial Wi-Fi streams
Power Input	<ul style="list-style-type: none">DC input: 12VPoE+

Physical	<ul style="list-style-type: none">• Dimension: 220 mm (W) x 220 mm (L) x 43mm (H)
Interfaces	<ul style="list-style-type: none">• 1 x 1/2.5 Gpbs Ethernet (PoE port)• 1 x 1 Gpbs Ethernet• 1 x DC jack for power supply (12V, 3A)• 1 x Reset to default button• 1 x Multi-color LED
Antenna	<ul style="list-style-type: none">• 4 x Integrated dual band Wi-Fi antennas
Button	<ul style="list-style-type: none">• Reset to Default
Environmental	<ul style="list-style-type: none">• Operating Temperature: 0°C to 50°C

8.2. Wi-Fi

Standards	<ul style="list-style-type: none">• 2.4Ghz 802.11b/g/n/ax• 5Ghz 802.11a/n/ac/ax
Radio Chains	<ul style="list-style-type: none">• 4 x 4
Spatial Streams	<ul style="list-style-type: none">• 4 for 2.4Ghz, 4 for 5Ghz
Performance	<ul style="list-style-type: none">• 2.4Ghz : 1.1Gbps• 5Ghz : 2.4Gbps
Maximum transmit power	<ul style="list-style-type: none">• 2.4 GHz: Up to 30dBm *1 (combined power)• 5 GHz: Up to 30dBm *1 (combined power)
Minimum receiver sensitivity	<ul style="list-style-type: none">• 2.4Ghz HT20/VHT20/HE20 : -95dBm @MCS0• 2.4Ghz HT40/VHT40/HE40 : -92dBm @MCS0• 5Ghz VHT20/HE20 : -97dBm @ MCS0• 5Ghz VHT40/HE40 : -94dBm @ MCS0• 5Ghz VHT80/HE80 : -91dBm @ MCS0
Max Number of Clients	<ul style="list-style-type: none">• Up to 128 per radio, so 256 if 2,4 and 5 GHz are used
ESSIDs	<ul style="list-style-type: none">• Up to 8

Our [General Terms and Conditions of Sale \(GTCS\)](https://www.microsens.com/fileadmin/files/downloads/Impressum/MICROSENS_AVB_EN.pdf) apply to all orders (see https://www.microsens.com/fileadmin/files/downloads/Impressum/MICROSENS_AVB_EN.pdf).

Disclaimer

All information in this document is provided 'as is' and is subject to change without notice.

MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or ensuing damage.

Any product names mentioned herein may be trademarks and/or registered trademarks of their respective owners.

©2022 MICROSENS GmbH & Co. KG, Kueferstr. 16, 59067 Hamm, Germany.

All rights reserved. This document in whole or in part may not be duplicated, reproduced, stored or retransmitted without prior written permission of MICROSENS GmbH & Co. KG.

Document ID: PM-22011_MS659150M-Indoor-Enterprise-Access-Point_User_Manual_v1.0